

1        SYSTEM AND METHOD FOR PROVIDING CONTEXT-AWARE COMPUTER  
2        MANAGEMENT USING SMART IDENTIFICATION BADGES

3

4            BACKGROUND OF THE INVENTION

5

6     1.    Field of the Invention

7            The present invention relates generally to systems and methods for context-aware  
8 computing, and more particularly for context-aware computer management using a smart  
9 badge.

10    2.    Discussion of Background Art

11           Context-aware computing is a field of computer science where computers are  
12 provided with sensors for detecting their orientation with respect to persons, places or  
13 things. Smart identification badges are an example of context-aware computing devices  
14 which contain an array of mini-sensors and wireless technologies for gathering  
15 information on their environment and communicating with other computers in order to  
16 provide such services as unlocking doors, and selective access to sensitive database  
17 information within various secure environments.

18           The mini-sensors can use a variety of biometric and standard technologies to  
19 monitor environmental conditions such as light, humidity, temperature, and sound levels,  
20 as well as spatial motions, voice patterns, and perhaps pheromones. Software programs  
21 then process this sensor information to conclude such things as who is wearing a smart  
22 badge and for how long. Researchers in the area of context-aware computing include Dr.  
23 Mark Smith at Hewlett-Packard Labs in Palo Alto and Gerald Maguire, professor of data  
24 communications at the Swedish Royal Institute of Technology.

1       Dr. Smith, for example, has developed a badge size SecurePAD which an  
2 employee picks up each morning, registers and authenticates in a secure booth, and  
3 carries on their person while at work. The badge communicates with beacons distributed  
4 throughout an office environment which respond to the badge by selectively opening  
5 doors and providing predetermined sets of information and functionality on secure  
6 computer systems. At the end of the day the badge is selectively inactivated. Presideo  
7 Inc., of Sebastian, Florida also manufactures similar security systems as described on  
8 their web site at <http://www.presideo.com>.

9           Figure 1 is a dataflow diagram of a prior art system 100 for interfacing with smart  
10 identification badges. In the system 100 credentials for several wearers are authenticated  
11 and downloaded into their respective smart badges 102, 104, 106, and 108. A computer  
12 110 connected to a narrow infrared (IR) beacon 112 selectively communicates with the  
13 badges 102-108. The beacon 112 by design has a short distance and narrow visibility  
14 range so that only one smart badge worn by an employee sitting right in front of the  
15 computer 110 is visible to the beacon 112 at any one time. The prior art considers this  
16 narrow range of visibility as a way to increase the system's 100 overall security.

17           A system service module 114 within the computer 110 communicates 111 with  
18 the smart badges through the beacon 112. When a first one 104 of the smart badges 102-  
19 108 becomes visible to the beacon 112, the service 114 queries the badge 104 for a set of  
20 credentials and, if the credentials are authentic, instructs the computer 110, perhaps using  
21 Microsoft Corporation's Graphical Identification and Authentication (GINA) 116 and OS  
22 Logon 118 modules, to log the employee carrying the badge 104 on to the computer 110.  
23 If the badge 104 is no longer visible to the beacon 112, the service 114 the GINA 116 to  
24 lock the computer 110 and blank the computer display even though the employee remains

1       logged on. Then, should the badge 104 become visible again, the service 114 instructs  
2       the GINA 116 to unlock the computer 110 and reactivate the computer display. If a  
3       second smart badge 106 becomes visible 120 to the computer 110, during a time when the  
4       first badge 104 is invisible to the beacon 112, the system service 114 instructs the GINA  
5       116 to log-off the employee assigned to the first badge 104, and log-on the employee  
6       assigned to the second badge 106.

7                  The system 100 is limited to allowing only one wearer to be logged on at any one  
8       time and requires that such wearer sit right in front of the computer 110 before unlocking  
9       the computer and display. Database security is thus achieved by logging only one wearer  
10      on a time. The wearer then runs a software application to access data in the database. The  
11      GINA's 116 role in controlling access to the database is by controlling which wearer logs  
12      on to the computer 110. In many operational settings, however, such an implementation  
13      is awkward to use. Furthermore, the prior art system 100 does not even begin to exploit  
14      the smart badge's 102-108 full capabilities for providing contextual information to the  
15      computer 110.

16                  What is needed is a system and method for context-aware computer management  
17      using a smart badge that overcomes the problems of the prior art.

18

1

## SUMMARY OF THE INVENTION

2       The present invention is a system and method for context-aware computer  
3       management. The method of the present invention includes the steps of: assigning  
4       database information one of several clearance levels; assigning each smart badge within a  
5       set of visible smart badges one of the clearance levels; identifying smart badges having a  
6       lowest clearance level; and providing access to database information having clearance  
7       levels no higher than the lowest clearance level.

8           In other aspects of the invention, the method may include the steps of: configuring  
9       a predetermined smart badge visibility range; updating the set of visible smart badges in  
10      response to a change in smart badge visibility status, and recalculating the lowest  
11      clearance level in response to the change in smart badge visibility status; recording the  
12      smart badge visibility status of each smart badge within an activity log; preventing  
13      database access to smart badge wearers when the wearer's smart badge visibility status is  
14      set to invisible longer than a predetermined timeout; reading and writing data items from  
15      and to the smart badges; defining a badge removal confidence level indicating whether  
16      each smart badge has been continuously worn by corresponding assigned smart badge  
17      wearers; assigning a smart badge time-to-live parameter to each of the smart badges; and  
18      inactivating a smart badge whose time-to-live parameter has been exceeded.

19          The system of the present invention includes a database storing information  
20      differentiated by a plurality of clearance levels; a wide-angle RF beacon; a set of smart  
21      badges, in communication with the beacon, each badge assigned one of the clearance  
22      levels; a system service module, connected to the beacon, for identifying a lowest  
23      clearance level assigned to the smart badges; and a software application, connected to the  
24      service module and the database, for providing access to information within the database

1 having clearance levels no higher than the lowest clearance level.  
2 In other aspects of the invention, the system may include a second diffuse IR  
3 beacon, coupled to the service module, for location awareness and perhaps limited to  
4 detecting smart badges within a workroom; the smart badges may also include biometric  
5 sensors for detecting when a smart badge has been removed from an assigned smart  
6 badge wearer.

7 The system and method of the present invention are particularly advantageous  
8 over the prior art because a customizable software application provides access to  
9 information based on clearance levels of those smart badge wearers visible to the  
10 beacons. Also, the wide angle first beacon enables the service module to monitor and  
11 communicate with all smart badges within a predefined area instead of just those smart  
12 badge wearers very close to or in front of the system.

13 These and other aspects of the invention will be recognized by those skilled in the  
14 art upon review of the detailed description, drawings, and claims set forth below.

15

1

BRIEF DESCRIPTION OF THE DRAWINGS

2       Figure 1 is a dataflow diagram of a prior art system for interfacing with smart  
3       identification badges;

4       Figure 2 is a dataflow diagram of an embodiment of a system for context-aware  
5       computer management using smart badges; and

6       Figure 3 is a flowchart of an embodiment of a method for context-aware computer  
7       management using smart badges.

8

PRINTED IN U.S.A. BY RICOH COMPANY, LTD.  
RICOH COMPANY, LTD.

1                   DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

2                  Figure 2 is a dataflow diagram of an embodiment of a system 200 for context-  
3                  aware computer management using smart badges. The system 200 includes a computer  
4                  202 coupled to a first wireless beacon 204, a second wireless beacon 206, and a database  
5                  208. The system 200 also includes one or more smart badges 210, 212, 214, and 216 in  
6                  communication with the computer 202 through the beacons 204, 206. The computer 202  
7                  may or may not be networked with other computers in a client/server topology.

8                  The smart badges 210-216 are context-aware devices which improve upon a  
9                  design developed by Dr. Mark Smith at Hewlett-Packard Labs in Palo Alto called  
10                 SecurePad. The badges communicate with the beacons 204, 206 using either Radio  
11                 Frequency (RF) and/or Infrared (IR) technology. The badges contain various biometric  
12                 and other sensors for detecting and monitoring the badges' surroundings, including those  
13                 persons wearing and/or objects affixed to the badges. While the following specification  
14                 discusses an embodiment of the present invention where the badges are worn by people in  
15                 a workroom, those skilled in the art will recognize that the present invention in other  
16                 embodiments can be used in a variety of other applications.

17                 The smart badges are preferably activated, and initialized within a standard  
18                 security booth. Within the booth a smart badge wearer follows a traditional security  
19                 protocol (i.e. such as typing a password on keyboard, or displaying a finger print) to  
20                 activate and initialize a badge. As part of initialization all smart badge credentials are  
21                 reset, previously stored data is erased, and a new set of data may be downloaded into a  
22                 data storage area within the smart badge.

23                 The first beacon 204 includes a transmitter and a receiver for establishing a  
24                 communications link between the computer 202 and the smart badges 210-216. The first

1 beacon 204 is preferably a wide angle device which can simultaneously detect and  
2 communicate with several smart badges. The first beacon 204 preferably communicates  
3 with the smart badges using an RF signal. RF signals can pass through walls, doors, file  
4 cabinets and other blocking objects and thus provides a more reliable communications  
5 link than IR. The second beacon 206 is preferably a diffuse IR device which works in  
6 conjunction with an RF first beacon 202. Since walls, doors, window, and etc. block IR  
7 signals, the second beacon 206 helps the computer 202 distinguish between smart badges  
8 within the workroom and smart badges passing by in a hallway outside of the workroom.

9           The database 208 preferably stores information having a plurality of  
10 confidentiality levels. Each smart badge wearer may have one of several different  
11 clearance levels assigned to their smart badge during the activation and initialization  
12 procedure. For example, if the information includes confidential patient medical records  
13 within a hospital setting, a first smart badge wearer, who is a doctor, may have a  
14 clearance level permitting accessibility to a first set of records and/or fields in the  
15 database 208, while a second smart badge wearer, who is a nurse, may have a clearance  
16 level permitting accessibility to a second set of records and/or fields in the database 208,  
17 which may or may not overlap with the first set of records and fields. Those skilled in the  
18 art recognize that the information in the database 208 could alternatively be business  
19 records in a corporate setting, financial records at a bank, or any other type of  
20 information.

21           While the entire system 200 is preferably located within the workroom, only some  
22 sort of user interface (e.g. a display terminal and a keyboard) and the second beacon 206  
23 need to be located within the workroom.

24           Within the computer 202 there is a system service module 218, an activity log

1 220, and a software application module 222. The computer 202 is initially and preferably  
2 booted up by a trusted system administrator, after which the system service 218 is  
3 automatically activated as a background process. The system administrator then logs on  
4 to the computer 202 using standard logon procedures. Once logged on, the administrator  
5 launches the software application 222.

6       The service module 218 is coupled to the first beacon 204, the second beacon 206,  
7 the activity log 220 and the software application 222. Software within the service module  
8 218 normally operates as an ongoing background process responsive to entry and exit of  
9 smart badges from the workroom. Those skilled in the art will recognize that while the  
10 system service 218 is described with reference to a Microsoft Corporation Windows NT  
11 environments consisting of background services, functionality within the system service  
12 218 module could easily be implemented by demons within a UNIX environment, or in  
13 another application program. Throughout operation, the service module 218 continually  
14 records and updates a variety of context-aware information in the activity log 220  
15 regarding the smart badges 210-216, their status, and configuration.

16       The application 222 provides database 208 access to only a predetermined set of  
17 smart badge wearers. The application 222 also includes database management code for  
18 selectively retrieving and displaying sets of records and/or fields within the database 208  
19 corresponding to the clearance level of each smart badge wearer within the workroom.  
20 The application 222 also may provide differing levels of software application  
21 functionality based on the clearance levels. Thus, the application provides data access  
22 security by cooperating with the system service 218 and consulting the activity log 220  
23 for a list of wearers present within the workroom and their corresponding clearance  
24 levels. Preferably, the wearers are not actually logged on and off of the computer 202,

1 but rather are either provided or denied access to the database 208 and functionality on  
2 the computer 202.

3 Returning to the hospital setting example, when the doctor is in the workroom, the  
4 application 222 permits retrieval and display of the first set of records and fields,  
5 however, should the nurse enter the workroom, the application 222 preferably permits  
6 retrieval and display of those records and fields which are common to the first and second  
7 sets of records and fields. Later, should a receptionist enter the workroom who does not  
8 have clearance to see any of the records or fields, the application 222 may deny access to  
9 all records and fields, and blank the computer display, even though the doctor and nurse  
10 are still in the workroom. Those skilled in the art will recognize that when information is  
11 or is not retrievable and displayed depends upon each implementation of the software  
12 application 222.

13

14 Figure 3 is a flowchart of an embodiment of a method for context-aware computer  
15 management using smart badges. The method begins in step 302 where wearers enter a  
16 secure booth and authenticate their smart badge. During authentication, the smart badge  
17 is reset to an initial state. Resetting the badge erases all prior credentials and stored data.

18 In step 304, the service module 218 configures the beacons 204, 206 to a  
19 predetermined smart badge field of visibility. While preferably, smart badge visibility is  
20 defined as those smart badges which are in communication with both beacons 204 and  
21 206, smart badge visibility range can also be adjusted by limiting transmitter power or  
22 receiver sensitivity of the smart badges 210-216, the first beacon 204, and/or the second  
23 beacon 206. In this latter, less favored implementation, first, the first and second  
24 beacons' 204, 206 transmitter output and the receiver sensitivity of the smart badges 210-

1       216 are all set at their maximum to ensure that the computer 202 can send commands to  
2       the smart badges 210-216. Then smart badge visibility is limited through predetermined  
3       adjustments to the beacons' 204, 206 reception sensitivity and/or the smart badges' 210-  
4       216 transmitter power.

5              In step 306, the service module 218 establishes communications with all visible  
6       smart badges. As discussed before, the smart badges 210-216 which are visible are  
7       preferably all located somewhere within the workroom.

8              Next in step 308, the service module 218 configures each of the visible smart  
9       badges. As part of configuration, the service module 218 defines a VisibleTimeout  
10      variable which specifies a predetermined period of time during which one or more of the  
11      smart badges can be invisible to (i.e. out of communication with) one or more of the  
12      beacons 204, 206.

13              The service module 218 can also set a variety of other smart badge variables, such  
14      as a TimeToLive variable, a LostBadgeTimeout variable, as well as internal clock and  
15      calendar variables. The TimeToLive variable sets an expiration period for the smart  
16      badge, which upon expiration, the smart badge automatically de-authenticates itself and  
17      erases all internally stored data. Preferably, the TimeToLive variable is set to a little  
18      longer than a standard work day.

19              The LostBadgeTimeout variable, specifies a time before the smart badge sounds  
20      an audible alarm, such as a beep, once the biometric sensors in the smart badge determine  
21      that the badge is no longer on the wearer. Preferably the LostBadgeTimeout variable is  
22      set to one hour.

23              In step 310, when a smart badge is no longer visible the service module 218  
24      changes that smart badge's status to invisible in the activity log 220 and sends a smart

1 badge timeout message to the application 222. The VisibleTimeout variable permits  
2 badge wearers to walk throughout the workroom and be invisible for a predetermined  
3 period of time without being identified within the activity log 220 as invisible. Preferably  
4 the VisibleTimeout predetermined period of time is set to five seconds.

5 In step 312, every 500 msec or so the service module 218 sends out a general  
6 transmit heartbeat command to all smart badges within the workroom. In response, each  
7 smart badge transmits a heartbeat status message to the service module 218, which is  
8 received by the service module 218 in step 314.

9 The heartbeat status message includes a predetermined set of badge status  
10 information, such as: smart badge identification (ID) number; badge removal confidence;  
11 badge removed; time-to-live; reset state; activation state; initialization state; badge  
12 activated; badge initialized; ID card on badge; ID card removed at least once; and battery  
13 state of charge. Note, the ID card is preferably a standard employee site badge. During  
14 authentication, wearers are required to insert their ID card in a slot on top of their smart  
15 badge. A sensor on the smart badge detects whether the ID card remains in the slot.  
16 Those skilled in the art will recognize that many other codes may also be included in the  
17 heartbeat.

18 The smart badge ID number is unique and permanently stored within each smart  
19 badge. The badge removal confidence is a variable which indicates a confidence level  
20 that the smart badge has been continuously worn by the smart badge wearer. Badge  
21 removal confidence is programmed by the smart badge's biometric sensors to between "0  
22 to 7," where "0" indicates with certainty that the badge was worn at all times by the  
23 wearer, and "7" indicates with certainty that at some time the badge was worn by a  
24 different wearer.

1        In step 316, the service module 218 stores each smart badge's heartbeat status and  
2    status changes in the activity log 220. Smart badge status changes include smart badge  
3    wearer enters the workroom, smart badge wearer leaves the workroom, and heartbeat  
4    status changes.

5        In step 318, the service module 218 responds to requests from the software  
6    application 222 for information stored within the activity log 220. In step 320, the  
7    software application 222 selectively displays information on the computer display in  
8    response to the activity log information and the application's 222 programming. In step  
9    322, the software application 222 also selectively provides functionality on the computer  
10   202 in response to the activity log information and the application's 222 programming.  
11   In step 324, the service module 218 updates the activity log 220 as smart badge status  
12   changes.

13        In step 326, the service module 218 read and/or writes binary data from/to the  
14   smart badge in response to commands from the application 222. Data items may include  
15   security passwords/cookies and/or other wearer specific personalized data. The data is  
16   preferably password protected and communication between the service module 218 and  
17   the smart badge can be either synchronous or asynchronous. Asynchronous data transfer  
18   tolerates a momentary loss of smart badge visibility during data transfer, such as when  
19   wearer moves about the workroom.

20        In step 328, the service module 218 periodically pre-reads a predetermined set of  
21   frequently used data from the smart badges. Pre-reading is defined as when the service  
22   module 218 reads data items from the smart badge during otherwise idle times when the  
23   badge is visible to the beacon 204, but no communications between the service module  
24   218 and the badge are otherwise required. The pre-read function enables the software

1 application 222 to be more responsive.

2 In step 330, the service module 218 selectively deletes data items from the smart  
3 badge in response to application 222 commands.

4

5 While one or more embodiments of the present invention have been described,  
6 those skilled in the art will recognize that various modifications may be made. Variations  
7 upon and modifications to these embodiments are provided by the present invention,  
8 which is limited only by the following claims.